PATENT ABSTRACTS OF JAPAN

(11)Publication number : 01-163871
(43)Date of publication of application : 28.06.1989

(51)Int.Cl. G06F 15/21
G06F 15/22
H04L 9/00
H04L 23/00

(21)Application number : 62-321220
(22)Date of filing : 21.12.1987

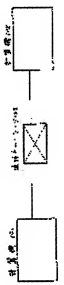
(71)Applicant : HITACHI LTD
(72)Inventor : GOTOU YASUKO
TAKARAGI KAZUO
SASAKI RYOICHI

(54) HIERARCHIZATION SYSTEM FOR SLIP COMPRESSED SENTENCE

(57)Abstract:

PURPOSE: To smooth an electronic transaction through an information network by enabling a slip confirmation by a segment-wise compressed sentence by the completion stage of a transaction, enabling to detect the falsification of a slip and enabling a unique digital signature reflecting a slip content.

CONSTITUTION: An electronic transaction is executed between computers 101 and 102 connected by a network 103. A slip prepared here is divided into some segments, data to be the point of a transaction are included in each divided segment, a compressed sentence is prepared for each segment, a compressed sentence including the content of the compressed sentence for each segment is prepared and it turns to be a representative compressed sentence in a transaction slip. The representative compressed sentence is used for a digital signature in the electronic transaction and the compressed sentences of each segment are preserved for the false detection of a slip falsification and the like. Thus, such electronic transaction such as the signing and sealing of contracts with the use of a computer can be attained.



⑲日本国特許庁（JP）　⑫特許出願公開

⑫公開特許公報（A）　平1－163871

⑤Int. Cl.⁴	識別記号	庁内整理番号	⑬公開　平成1年(1989)6月28日
G 06 F 15/21 15/22		Z－7230－5B 7230－5B	
H 04 L 9/00 23/00		A－7240－5K A－7240－5K	審査請求　未請求　発明の数　1　（全4頁）

⑭発明の名称　伝票圧縮文階層化方式

⑳特　願　昭62－321220
㉒出　願　昭62(1987)12月21日

㉑発明者　後藤　寧子　神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
㉑発明者　宝木　和夫　神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
㉑発明者　佐々木　良一　神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
㉑出願人　株式会社日立製作所　東京都千代田区神田駿河台4丁目6番地
㉔代理人　弁理士　小川　勝男　外1名

明　細　書

1．発明の名称

伝票圧縮文階層化方式

2．特許請求の範囲

1．電子取引において、相手評価、および取引内容（伝票）の確認を行なうために用いる取引者同士が必要とする伝票の圧縮文作成において、該伝票の全部あるいは一部をいくつかに分割し、かつ分割した各部位には、取引伝票におけるポイントとなるデータを含め、該分割部位毎に、圧縮文を作成し、部位毎の該圧縮文から、該伝票内容を反映した一意的な代表圧縮文を作成し、該代表圧縮文を用いてディジタル署名を行うことにより、取引の終了段階までに、部位別圧縮文による伝票確認を可能とするとともに、伝票の不正改ざん検知を可能とし、さらに伝票内容を反映した一意的なディジタル署名を可能とすることを特徴とする伝票圧縮文階層化方式。

3．発明の詳細な説明

〔産業上の利用分野〕

本発明は、情報ネットワークを介した電子取引に関する。

〔従来の技術〕

いま、通信ネットワークを介して、会社や様々の取引を電子的に行うビジネス通信の時代が始まろうとしている。近い将来、コンピュータを用いて契約書に署名、通帳するといった電子取引も実現するものと予想される。

公開鍵暗号を応用して作成されるディジタル署名は、電子取引において次の理論をもたらすものとして注目されている。

(1) 送信者は、通信事実、および通信内容を否定することができない。

(2) 受信者は、通信事実、および通信内容を否定することができない。

これにより、ディジタル署名は従来の印鑑に相当する機能をデータ通信において実現し得るものと期待されている。

〔発明が解決しようとする問題点〕

ところで、電子取引におけるディジタル署名は

取引伝票の圧縮文と取引状況を示す内容とから成り、取引伝票の圧縮文は、取引伝票の内容が１ビットでも異なれば全く別のものになるという厳めて感度の高いものである。

従って、不当に取引伝票を改ざんされた場合、本来できる４者圧縮文を改ざんされた伝票の圧縮文が異なり、伝票改ざんを証明することになる。

しかしながら、伝票を改ざんした事実を証明することは可能でも、伝票におけるどの部位を改ざんしたかを証明することは不可能であった。

（問題点を解決するための手段）

上記の問題点を解決するために、本発明では次の手段を用いる。

(1) 作成する伝票をいくつかに分割する。分割した各部位には、取引のポイントとなるようなデータを含ませる。

(2) 各部位等に圧縮文を作成し、各個位等の圧縮文の内容を含む圧縮文を作成し、これを取引伝票における代表圧縮文とする。

(3) 電子取引におけるディジタル署名には、代表圧縮文を用い、各部位の圧縮文は、伝票改ざん等の不正検知用として保存する。

（作用）

前記技術的手段により、次の作用が生じる。

1．不注意なミスによる不要な取引の減少

取引において、避けがたいヒューマン・エラーに対し、取引担当者も部位ごとの圧縮文作成及び圧縮文のチェックを行うことにより、ヒューマン・エラーを検知することができ、不必要な取引を行うことを避けることが容易になる。

2．取引伝票の不正な改ざん部位を検知

分割した伝票の各部位に、取引のポイントとなるデータ（例えば、株式売買においては、銘柄，株数，約例，売買等）を含ませることにより各部位毎における各部位圧縮文は、各ポイントデータを反映するものと考えられるので、改ざん部位を推定することが容易になる。

3．伝票内容を反映したディジタル署名

部位圧縮文全てを入力データとして作成した代表圧縮文をディジタル署名の原文とすること

により、ディジタル署名は、伝票内容を反映した一意的なものとして実現することも可能である。（実施例）

以下、本発明の一実施例を、第１図，第２図により説明する。第１図に示すネットワークで結ばれた二者間において電子取引を行う。

step１：計算機１０１、あるいは１０２において、取引伝票２０１は、所定の規約に従って、Ｍ１（２０２），Ｍ２（２０３），Ｍ３（２０４），Ｍ４（２０５）の４部位（ここでは４部位とする）に分割する。

Ｍ１の部位データには、銘柄データを含ませ、

Ｍ２の部位データには、約買データを含ませ、

Ｍ３の部位データには、株数データを含ませ、

Ｍ４の部位データには、価格データを含ませる。

step２：分割した部位データＭ１～Ｍ４について、各々のデータから部位圧縮文ＭＡＣ１～ＭＡＣ４を計算機１０１（あるいは１０２）上で作成する。圧縮文作成方式については後述する。

step３：部位圧縮文ＭＡＣ１～ＭＡＣ４を基に、取引伝票２０１の代表圧縮文ＭＡＣを計算機101（あるいは１０２）において、作成し、ＭＡＣおよびＭＡＣ１～ＭＡＣ４を伝票２０１の圧縮文データとする。

step４：計算機１０１（計算機１０２）において、作成して圧縮文と伝票データを通信ネットワーク１０３を介して、計算機１０２（計算機１０１）に送信し、以下電子取引（電子振込)文書）を行う。

step５：計算機１０２（計算機１０１）では、同様に部位圧縮文と代表圧縮文を作成し、取引伝票のチェックを行う、ここで、不当な伝票作成ミス等の検知を行う。

step６：計算機１０２（あるいは１０１）において、電子署名交換を行う際、代表圧縮文を用いてディジタル署名を行い、電子取引を行う。

step７：書引後、計算機１０１と１０２個において、くい違いが生じた場合、生成する伝票の部位圧縮文、および、代表圧縮文を作成し、比較することにより、伝票データの不正な改ざん検知と改ざん部位の推定を行う。

圧縮文作成は、取引伝票Mを５６ビット先のブロックに区切り、各ブロックをＭ１，Ｍ２，…Ｍｎとする。最後のＭｎが５６ビット長に満たない時は、"０"を付加し、補正する。

前記ブロックに対し、７ビット単位で１ビットのパリティ・ビットを付加し、ブロック長を６４ビットに拡張し、これをＫ１，Ｋ２…Ｋｎとする。

入力データＩ（ｉ－１）を鍵Ｋｉで暗号化（Ｅ）したものとＩ（ｉ－１）との非線的論理和をとったものをＩ（ｉ）とする。

Ｉ(ｉ)＝Ｉ（ｉ－１）⊕ＥＫｉ(Ｉ（ｉ－１))

以上の処理を、ｉ＝１，２…について行う。また、初期値Ｉ（０）は、予め定められた値だとする。ただし⊕は、ビット対応の非線的論理和を表す。

最終的に求められた値Ｉ（ｎ）が圧縮文となる。

補部部位圧縮文は、取引伝票Ｍの一部から作成するものである。

実施例の変形例１

伝票の分割方法は必要と要求に応じて、均等分割，レベル別分割、あるいは、おりふり分割等を行うことも可能である。また分割は、伝票全体，あるいは一部に対して行うことも可能である。

実施例の変形例２

部位圧縮文は、部位毎に独立のものとすることも、あるいは、部位Ｍ１の圧縮結果を部位Ｍ２が包括し、部位Ｍ３は部位Ｍ２の圧縮結果を包括するものとすることも可能である。

【発明の効果】

１．不正変造ミスによる不要な取引の減少。

取引において、避けがたいヒューマン・エラーに対し、取引段階で各部位毎の圧縮文作成、及び部位圧縮文のチェックを行うことにより、ヒューマン・エラーを検知することができ、不必要な取引を行うことを避ける。

２．伝票改ざん部位を検知

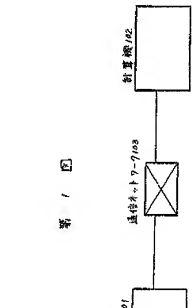
分割した伝票の各部位に、取引のポイントとなるデータ（例えば、株式売買においては、指値，株数，銘柄，売買等）を含ませることにより、各部位毎における部位圧縮文は、各ポイントデータを反映するものと考えられるので、改ざん部位を推定することが容易にできる。

３．伝票内容を反映したディジタル署名

各部位圧縮文を入力データとして作成した代換圧縮文をディジタル署名の原文とすることにより、ディジタル署名は、伝票内容を反映した一意的なものとして実現することも可能である。

４．図面の簡単な説明

第１図は本発明を実施する電子取引システムの構成例を示すブロック図、第２図は本発明の電子取引における伝票の圧縮的圧縮文作成のための、標式処置を施した伝票の分割例を示す説明図である。



第１図

代理人　弁理士　小川勝男

特開平1-163871(4)

第 2 図